Issue 40

April 2013

Page 1 of 2

M & H CONSULTING

THE M&H MONITOR

Password Policy: Your First Line of Defense

Tim Clarkin

With new more stringent data security laws and newer more complex threats from viruses and hackers, one of the most important barriers between your business and major problems is instituting a strong password policy across the board. Too often, individuals and organizations have issues that can be caused from either not rotating passwords, password sharing across multiple accounts, failing to require complexity in the passwords, or even having no password at all. This can leave systems subject to being hijacked by spammers, being more susceptible to malware infections, compromised by malicious persons looking to wreak havoc on a network, or simply leave you vulnerable to legal and financial repercussions in the event of a data breach.

If an email account in your system were to be compromised, it could send out hundreds, if not thousands, of messages before the breach was noticed and would likely lead to the server being placed on a blacklist. Blacklists are tools designed to stop spammers by keeping track of spamming servers and blocking them until removed. This can cost time and money, and be a source of embarrassment for your organization.

Virus infections will typically also try to exploit the lack of a password on an account as a way to spoof the user's permission to load in more infections, send out spam email and even steal data. In addition to that, having older unchanged passwords could allow a disgruntled former employee to gain access to information so they can manipulate, delete, or even share confidential and important data. Again, this can cause downtime, as well as potentially leaving you vulnerable to further penalties due to industry and state specific regulations.

So what can you do to prevent these kinds of issues? Implementation of a strong password policy is the easiest way to be sure you're limiting your potential risk factors. A strong password, as defined by Microsoft, is one that is at least seven characters or more including at least one upper and lower case letter, one number, and one symbol. Ideally, dictionary words should be avoided (even if they're just part of the password) and the password should not be conforming to a scheme for all users that would allow knowing one password make others less secure. Conforming to these statuses dramatically increases anyone being able to guess the password either through basic logic or with a "dictionary attack" where an automated program will keep guessing patterns. Password sharing and or having passwords publicly displayed in an office (i.e. a post-it note in on a monitor) should be strictly avoided. Passwords should be rotated in regular intervals (at minimum 1-2x per year, depending on the type of data access) and when an employee leaves, any passwords that he or she may have had access to should also be changed. Any setup where multiple user accounts are using the same password should also be avoided proactively in advance, so as to prevent a situation where one employee leaving requires everyone to change their password.

Certain industries (financial and healthcare, in particular) may be subject to stricter regulations, but following those basic guidelines helps your organization to avoid unnecessary and preventable headaches. As with any "best practices", they certainly are not 100% foolproof, but you will put your organization in the best position to not get bogged down with problems that could have been easily prevented with a proactive approach to security. If you have questions about passwords on your systems, contact us anytime at 866-9MH-TECH or email us at support@mhconsults.com.

Backing up your data

Anyone who has ever lost files after a computer crash knows it is important to back up your data. But how should you back it up? What are the differences in cost and features between different methods of backup? What should you use for your business or home computer? What data should you back up?

On-site/Local file backup

The traditional method for backing up data is to use a program or script on your computer/server to back up your data onto some local storage media. This method can be more expensive, depending on the software & hardware that are used, and it sometimes requires more maintenance than online backups. The benefits of a local backup are that it can allow for greater depth and flexibility for retaining backups and archives, and it also allows you to keep all of your data in-house.

Examples of backup software used for local backups are: Symantec Backup Exec, NTBackup (the built-in Windows backup program), and backup scripts. Simply copying and pasting files is another option, but most users find this too cumbersome to do repeatedly. Examples of local backup media include secondary internal hard drives in a PC, CD's/DVD's, external USB hard drives, flash drives, or backup tapes.

Off-site/Online file backup

Online backup programs are becoming more and more popular. These are subscription-based services, and they work by running a program on your computer that copies your data to a secure server hosted elsewhere on the Internet. Online backups are generally easy to use, and are most are highly reliable. The fact that the data is stored off-site means that even if a disaster destroys your machine(s), you should still be able to recover your data. There is a wide range of online backups available, with a wide range of features and prices. Most online backup companies offer different plans based on the total storage you need.

Examples of online backup products are: Mozy, Crashplan, Carbonite, IBackup, and Venyu.

What to back up?

The most common approach is to use a simple file backup. Many backup programs will actually select most of your important files by default (Desktop, My Documents, etc.); however, it is important to actually check and make sure everything is selected.

A more "complete" approach is to use an imaging solution. An imaging program will actually take a "snapshot," not only of your files but of the complete system state. The advantage of this would come in the event of a hard drive failure. If a replacement hard drive were installed in the same machine, the image backup could be used to restore the system back to its previous state (instead of having to fully reinstall Windows, reinstall all programs, and reconfigure all settings). Imaging programs are generally more expensive than simple file backups, and there are some limitations to the usability of backup images.

Issue 40

April 2013

Page 2 of 2

THE M&H MONITOR

M&H CONSULTING

eMachines Class-Action Lawsuit

Jeff Fanning

Have you owned an eMachines computer anytime in the last 16 years? If that computer had a floppy drive in it, you may be eligible to receive benefits from a settlement being reached in a class action suit.

The lawsuit, known as Stroud v. eMachines, Inc., claimed that the defendants sold computers with a defective part that could possibly cause the loss or corruption of data. Both parties have agreed to a settlement in order to avoid further litigation, with a final approval hearing scheduled for March 25, 2013.

Class members will have the option to receive a redemption certificate worth $365 which can be used to purchase a replacement computer from Acer, Gateway, or eMachines. The other options for Class Members are receiving a sum of $62.50 in cash and/or accessories.

The models included were sold on or after December 31, 1997, and are as follows:

eTower Models: 266, 300c, 300K, 333c, 333cs, 333k, 366c, 366i, 366id, 366is, 366i2, 400i, 400i2, 400ix, 400id, 400idx, 400i3, 433i, 466i, 466id, 466is, 466ix, 500i, 500idx, 500is, 500ix, 500ix2, 533i, 533id, 533ir, 533id2, 566i, 566i2, 566ir, 566irx, 600ix, 600id, 600is, 633id, 633irx, 633ids, 667ix, 667ir, 700, 700irs, 700irx, 700id, 700ir, 700ix, 700k, 733i, 766, 766id, 800.

eMonster Models: 500A, 500, 500a, 550, 550r, 600, 700K, 800, 1000, 1000B.

T Models: 1090, 1096, 1100, 1105, 1106, 1110, 1801, 1855, 1905, 3100.

As with any Class Action Lawsuit, time is of the essence. Below are the important dates and deadlines.

Deadline for filing a claim: Postmarked by July 15, 2013.

You must complete and submit a Claim Form by July 15, 2013. You must also provide documents such as Proof of Purchase and all of the information the Claim Form requires. For more information on Claim Forms and your rights in the eMachines Class Action Lawsuit Settlement, please visit:

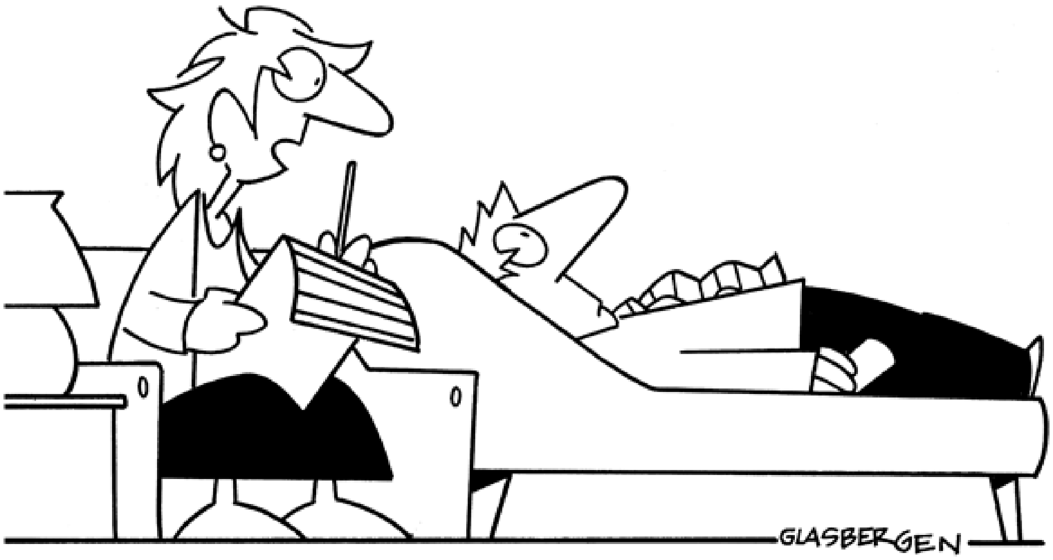
www.eMachinesFloppyDiskSettlement.com.

If you want to retain the right to sue the Defendants about this issue, and you do not want the benefits provided in the Proposed Nationwide Settlement, you must exclude yourself from it. To do this, you must send a letter by mail requesting exclusion from the Class Action. Detailed instructions for doing so are listed at the website shown above.

If you have questions about this or need help determining whether you might be eligible to receive benefits, contact us today at 866-9MH-TECH, or email us at support@mhconsults.com.

TAKE $$$CASH$$$ FROM M&H CONSULTING

Refer a new Tech-For-A-Day client to M&H Consulting and mention this offer to us, and you will receive $25 for each PC the new client has. Call for details.



"Shut off your cell phone, GPS, iPod and Bluetooth headset, then let me know if you still hear the voices."

If you would like to be removed from this newsletter, send an email to info@mhconsults.com with the word "remove" in the subject line.